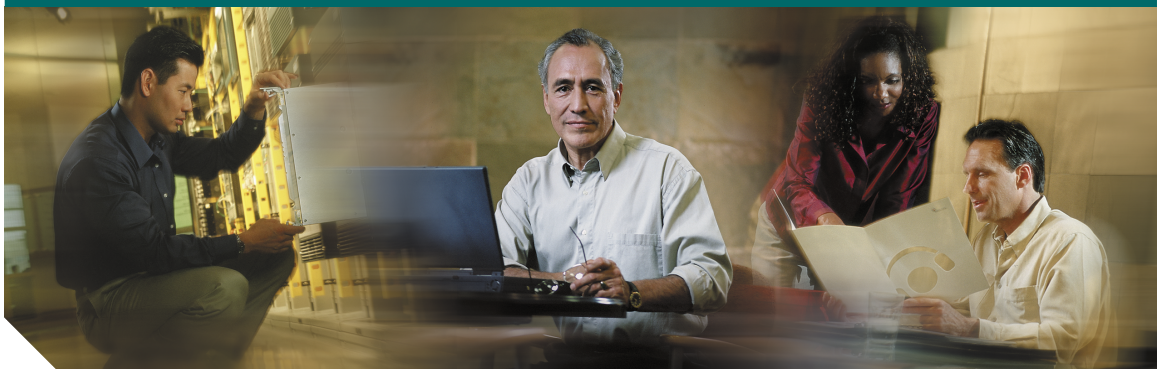
Quick Start Guide



Cisco Intrusion Detection System Version 4.1

1 Product Summary
2 System Requirements and Upgrade Notes
3 How to Obtain Product Updates
4 Installing Your Sensor
5 Information You Need Before You Configure the Sensor
6 Products You Can Use to Configure Your Sensor
7 Products You Can Use to View Events
8 Where to Go for More Information

1 Product Summary

Cisco Intrusion Detection System (IDS) Version 4.1 software includes support for the new IDS-4215 appliance and the IDS network module for Cisco 2600/3600/3700 series routers. Version 4.1 ships with an updated version of the IDS Device Manager that includes enhanced support for signature configuration with a new Signature Wizard. You can also download an updated version of IDS Event Viewer that includes enhanced support for viewing captured packets.

2 System Requirements and Upgrade Notes

System Requirements

Cisco IDS Appliances

- Supported Cisco IDS Software:

  Cisco IDS software release 4.0 or later

- Supported Platforms:

  IDS-4250-TX-K9, IDS-4250-SX-K9, IDS-4250-XL-K9, IDS-4235-K9, IDS-4230-FE, IDS-4220-E, IDS-4215-K9, IDS-4215-4FE-K9, IDS-4210, IDS-4210-K9, IDS-4210-NFR

Note To qualify as a supported platform, the IDS-4220-E, IDS-4210, IDS-4210-K9, and IDS-4210-NFR platforms must have the supported memory upgrade (Part Number IDS-4210-MEM-U or IDS-4220-MEM-U). For detailed memory upgrade instructions, please read the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

Services Module for Cisco Catalyst 6500 Series Switches

Note The operating system versions specified are the earliest versions on respective release trains that support IDSM2.

- Supported Catalyst Software:

  Catalyst software release 7.5(1), 7.6(1), or later with any supervisor engine
- Supported Cisco IOS Software:

  Cisco IOS software release 12.2(14)SY with supervisor engine 2 with MSFC2

  Cisco IOS software release 12.1(19)E with supervisor engine 2 with MSFC1 and supervisor engine 2 with MSFC2
- Supported Cisco IDS Software:

  Cisco IDS software release 4.0 or later
- Supported Platforms:

  Any Catalyst 6500 Series Switch chassis

Network Module for Cisco 2600/3600/3700 Series Routers

- Supported Cisco IOS Software:

  Cisco IOS software release 12.2(15)ZJ or later
- Supported Cisco IDS Software:

  Cisco IDS software release 4.1 or later
- Supported Feature Sets:

  IOS IP/FW/IDS

  IOS IP/FW/IDS PLUS IPSEC 56

  IOS IP/FW/IDS PLUS IPSEC 3DES

  IOS IP/IPX/AT/DEC/FW/IDS PLUS

  IOS ENTERPRISE/FW/IDS PLUS IPSEC 56

  IOS ENTERPRISE/FW/IDS PLUS IPSEC 3DES

  IOS Advanced Security

  IOS Advanced IP

  IOS Advanced Enterprise
- Supported Platforms:

  Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745

Upgrade Notes

You can upgrade from Version 4.0 to Version 4.1 by downloading the upgrades from Cisco.com. See How to Obtain Product Updates, page 5 for more information.

- For all sensors, you must assign the sensing interface(s) according to the following guidelines:
  - Interface group 0 is the only interface group supported. This interface group provides a way to group sensing interfaces into one logical virtual sensor. This functionality will be expanded to support multiple virtual sensors in future releases.
  - If your sensor shipped with version 4.1, the sensor detects the available sensing interfaces and adds them to interface group 0. If the XL interface is present, only the XL is added to interface group 0. By default, the interfaces are disabled. Before you can monitor traffic, you need to enable the appropriate interfaces. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the procedure.
  - If you are upgrading an existing sensor to version 4.1, the sensor detects the available interfaces. The IDS appliances retain the status of the interfaces. For example, an interface with a status of *enabled* at the time of upgrade is retained in interface group 0 as an enabled interface. However, an interface with a status of *disabled* at the time of upgrade is not retained in the group. You must add the unassigned sensing interfaces to interface group 0.
  - The IDSM-2 does not retain the status of the interface. For example, an interface with a status of *enabled* at the time of upgrade is retained in interface group 0, but is disabled by default. You must enable the sensing interfaces. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the procedure.
  - If you are currently using the Command and Control interface as the sensing interface, you will receive an error the first time IDS version 4.1 boots. The Command and Control interface is an invalid interface for interface group 0. You need to remove the invalid interface from interface group 0 and add a valid sensing interface.
- For the IDS-4220-E, IDS-4210, IDS-4210-K9, and IDS-4210-NFR platforms, you must use the supported upgrade (Part Number IDS-4210-MEM-U or IDS-4220-MEM-U) to upgrade the memory to 512 MB RAM. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the memory upgrade procedure.
- For the IDS-4220 and IDS-4230, you must swap the command and control interface cable with the sniffing interface cable before installing the version 4.0 or later software. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the procedure.
- For the IDS-4235 and IDS-4250, if your BIOS version is lower than A04, you must apply the BIOS upgrade before installing the version 4.0 or later software. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the BIOS upgrade procedure.

3 How to Obtain Product Updates

Apply for a Cisco.com Account with Cryptographic Access

To download software updates, you must have a Cisco.com account with cryptographic access.

If you do not have a Cisco.com account, register for one at the following site:
http://tools.cisco.com/RPF/register/register.do

Register for cryptographic access at the following site:
http://www.cisco.com/pcgi-bin/Software/Crypto/crypto_main.pl

Software Center

You can find IDS Event Viewer, signature updates, service pack updates, BIOS upgrades, and other software updates from Software Center on Cisco.com at the following URL:

Note You must be logged in to Cisco.com to access Software Center. If you are not logged in, the following URL will not work.

http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto

Register for Active Update Notification

You can subscribe to the Cisco IDS Active Update Notifications service to receive e-mails when signature updates and service pack updates occur. To sign up for the service, register at the following site:

http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html

After registering, you will receive e-mail notifications of updates when they occur and instructions on how to obtain them.

4 Installing Your Sensor

The following section highlights the basic installation options for the IDS appliances and modules. For detailed installation procedures, please read the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

⚠

Caution Be sure to read the Regulatory Compliance and Safety Information document that accompanied this device before installing the sensor. This document contains important safety information.

Appliances

IDS-4250-TX-K9, IDS-4250-SX-K9, IDS-4250-XL-K9

IDS-4235-K9

IDS-4230-FE

IDS-4220-E

IDS-4215-K9, IDS-4215-4FE-K9

IDS-4210, IDS-4210-K9, IDS-4210-NFR

Basic Installation Instructions for IDS Appliances

Step 1 Make sure that you take necessary safety precautions and read the Regulatory Compliance and Safety Information document that accompanied this device before installing the sensor. For detailed installation procedures, please read the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

Step 2 Position the IDS appliance on the network.

Step 3 Attach the power cord to the IDS appliance and plug it into a power source (a UPS is recommended).

Step 4 Connect the serial cable:

- For the 4215, use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit (PN 72-1259-01). The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

  Connect the RJ-45 connector to the console port and connect the other end to the serial port connector on your computer.

- For all other supported appliances, use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) to attach a laptop to the COM1 port of the IDS appliance.

- Use the following terminal settings:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: Hardware or RTS/CTS

Note You can use a 180/rollover or straight-through patch cable to connect the sensor to a port on a terminal server with RJ-45 or hydra cable assembly connections. For the IDS-4215, connect the appropriate cable from the console port on the IDS-4215 to a port on the terminal server. For all other sensors, use a M.A.S.H adapter (PN 29-4077-01) to connect the appropriate cable to a port on the terminal server. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1* for instructions on setting up a terminal server.

Step 5 Attach the network cables.

- For the 4215, INT0 is the monitoring port, INT1 is the command and control port, and INT2 through INT5 are the optional monitoring ports provided if you have the 4FE card installed.
- For the 4220/4230, the PCI card (int1) is now used as the command and control interface and the onboard NIC (int0) is used as the sniffing interface.

Step 6 Power on the IDS appliance.

You are now ready to configure your IDS appliance. Refer to the "Information You Need Before You Configure the Sensor" section on page 10.

Modules

- Services Module for Cisco Catalyst 6500 Series Switches

  WS-SVC-IDSM2-K9
  Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module
- Network Module for Cisco 2600/3600/3700 Series Routers

  NM-CIDS-K9
  Cisco Intrusion Detection System Network Module (NM-CIDS)

Basic Installation Instructions for the Services Module (IDSM-2)

All Catalyst 6500 series switches support hot swapping, which lets you install, remove, replace, and rearrange modules without turning off the system power. When the system detects that a module has been installed or removed, it runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation with no operator intervention.

Step 1 Make sure that you take necessary safety precautions and read the Regulatory Compliance and Safety Information document that accompanied this device before installing the sensor. For detailed installation procedures, please read the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

Step 2 Choose a slot for the module.

Note The supervisor engine must be installed in slot 1; a redundant supervisor engine can be installed in slot 2. If a redundant supervisor engine is not required, slots 2 through 9 (slots 2 through 6 on the 6-slot chassis and slots 2 through 11 on the 13-slot chassis) are available for modules.

Step 3 Loosen the installation screws (use a screwdriver, if necessary) that secure the filler plate to the desired slot.

Step 4 Remove the filler plate by pulling the ejector levers on both sides and sliding it out.

Step 5 Hold the module with one hand, and place your other hand under the module carrier to support it.

Caution Do not touch the printed circuit boards or connector pins on the module.

Step 6 Place the module in the slot by aligning the notch on the sides of the module carrier with the groove in the slot.

Step 7 Keeping the module at a 90-degree orientation to the backplane, carefully slide it into the slot until the notches on both ejector levers engage the chassis sides.

Step 8 Using the thumb and forefinger of each hand, simultaneously pivot in both ejector levers to fully seat the module in the backplane connector.

Caution Always use the ejector levers when installing or removing the module. A module that is partially seated in the backplane will cause the system to halt and subsequently crash.

Note If you perform a hot swap, the console displays the message `Module` *x* `has been inserted`. This message does not appear, however, if you are connected to the Catalyst 6500 series switch through a Telnet session.

Step 9 Use a screwdriver to tighten the installation screws on the left and right ends of the module.

You are now ready to configure your IDSM-2. Refer to the "Information You Need Before You Configure the Sensor" section on page 10.

Basic Offline Installation Instructions for the Network Module (NM-CIDS)

You can install the IDS network module in the chassis either before or after mounting the router, whichever is more convenient. Cisco 3660 and Cisco 3700 series routers allow you to replace IDS network modules without switching off the router or affecting the operation of other interfaces. Online insertion and removal (OIR) provides uninterrupted operation to network users, maintains routing information, and ensures session preservation (Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.* for the online procedure). You must install the IDS network module offline in Cisco 2650XM, 2651XM, and 2691 series routers.

Step 1 Make sure that you take necessary safety precautions and read the Regulatory Compliance and Safety Information document that accompanied this device before installing the sensor. For detailed installation procedures, please read the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.*

Step 2 Turn OFF electrical power to the router.

Step 3 Remove all network interface cables, including telephone cables, from the back panel.

Step 4 Using either a number 1 Phillips screwdriver or a small flat-blade screwdriver, remove the blank filler panel from the chassis slot where you plan to install the IDS network module.

Step 5 Align the IDS network module with the guides in the chassis and slide it gently into the slot.

Step 6 Push the module into place until you feel its edge connector mate securely with the connector on the motherboard.

Step 7 Fasten the IDS network module's captive mounting screws into the holes in the chassis, using the Phillips or flat-blade screwdriver.

Step 8 If the router was previously running, reinstall the network interface cables and turn ON power to the router.

The following warning applies to routers that use a DC power supply:

Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

5 Information You Need Before You Configure the Sensor

Logging In

To access the IDS CLI **setup** command:

- For the IDS appliances, use a serial connection.
- For the IDSM-2, session in to the services module:
  - For Catalyst software: Console> (enable) **session** *module_number*
  - For Cisco IOS software: Router# **session slot** *slot_number* **processor 1**
- For the NM-CIDS, session in to the network module:
  - Router# **service-module IDS-Sensor** *slot_number/port_number* session

The sensor is initially configured with the following administrator account:

username: cisco

password: cisco

You can use this account to initially log in to the sensor. However, the temporary password *cisco* expires upon initial log in. When prompted, you must change the password for this default account to a string that is not a dictionary word and is at least 8 alpha-numeric characters long. Special characters are not supported. From the administrator account, you can also add additional user accounts with viewer, operator, or administrator privileges.

Use the following checklist as a guide for gathering the information you will need before you initially configure your sensor. After you have the necessary information, access the IDS CLI and run the **setup** command to configure the initial settings. You can then use the products listed in Section 6 to complete the sensor configuration.

Checklist for Initial Sensor Setup

	Information You Need	Value
	For the Sensor (initial settings):	
	Hostname (case-sensitive; default is *sensor*)	
	IP Address (address of sensor; default is 10.1.9.201)	
	Network Mask (default for Class C is 255.255.255.0)	
	Default Route (default gateway is 10.1.9.1)	
	Enable Telnet services? (default is disabled)	
	Web Server Port (default is 443)	
	For All Hosts Allowed to Connect to Sensor (this includes monitoring applications, like the IDS Event Viewer):	
	IP Address	
	Network Mask	
	For All SSH Client Connections to Sensor:	
	IP Address	
	Key Modulus Length	
	Public Exponent	
	Public Modulus	
	For All TLS (Web Server) Connections to Sensor:	
	IP Address of Host with x.509 certificate	

6 Products You Can Use to Configure Your Sensor

IDS Device Manager

IDS Device Manager is a web-based application that allows you to configure and manage your IDS sensor. The web server for IDS Device Manager resides on the sensor. Using secure HTTP, you can access it through Netscape or Internet Explorer web browsers by typing in the IP address of the sensor. The default web server port is 443. If you change the web server port, you must specify the port in the URL address in the format https://*sensor ip address*:`port` when you connect to IDS Device Manager (for example, https://10.1.9.201:1040).

For detailed information on using the IDS Device Manager refer to *Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1*.

Management Center for IDS Sensors

Management Center for IDS Sensors (IDS MC) manages configurations for up to 300 IDS sensors. You use a series of web-based screens to manage all aspects of sensor configuration. You can manage individual sensors, and you can manage groups of sensors having a common configuration. The sensor configuration data resides in a database. You must install CiscoWorks before installing IDS MC.

For detailed information on using the IDS MC, refer to *Using Management Center for IDS Sensors 1.1*.

Cisco Intrusion Detection System 4.1 Command Line Interface

The command line interface for Cisco Intrusion Detection System 4.1 (IDS CLI) allows Telnet, SSH, and serial interface connection to the sensor.

For a detailed information on using the IDS CLI, refer to the *Cisco Intrusion Detection System Command Reference Version 4.1* and *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1*.

7 Products You Can Use to View Events

IDS Event Viewer

IDS Event Viewer is a Java-based application that enables you to view and manage alarms for up to five sensors. With IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis. IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

You can download IDS Event Viewer from the following site:

http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev

For detailed information on using the IDS Event Viewer, refer to *Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1*.

Monitoring Center for Security

Monitoring Center for Security (Security Monitor), provides event collection, viewing, and reporting capability for network devices. You must install CiscoWorks before installing Security Monitor.

For detailed information on how to use the Security Monitor, refer to *Using Monitoring Center for Security 1.1*.

8 Where to Go for More Information

To locate related documentation on Cisco.com,

- For Cisco IDS version 4.1, select:
  - Products & Services > Security and VPN Software > Cisco Intrusion Detection System > Technical Documentation.
- For IDS MC, select:
  - Products & Services > Network Management CiscoWorks > CiscoWorks Monitoring Center for Security > Technical Documentation
  - Products & Services > Network Management CiscoWorks > CiscoWorks Management Center for Security > Technical Documentation
- For Cisco 2600/3600/3700 Series routers and network modules, select:
  - Products & Services > Cisco Interfaces and Modules > Cisco Network Modules > Technical Documentation
  - Products & Services > Cisco Routers > 3700 series > Technical Documentation.
- For Catalyst 6500 Series switches, select:
  - Products & Services > Cisco Switches > Cisco Catalyst 6500 > Technical Documentation.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

©2004 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSI, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Printed in the USA on recycled paper containing 10% postconsumer waste.
78-15594-02
DOC-7815594=